IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

CARRIE KOVAL-BURT, individually, and on behalf of all others similarly situated, Plaintiff, v. HAMILTON BEACH BRANDS, INC., Defendant.	)	Civil Action No. **3:21-cv-00274-DJN** JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Carrie Koval-Burt ("Plaintiff") brings this Class Action Complaint against Defendant Hamilton Beach Brands, Inc. ("Hamilton Beach" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Hamilton Beach is a manufacturer and retailer of household and kitchen appliances. While Hamilton Beach sells its products at major stores throughout the United States, it also does so on its own website.

2. On or about April 9, 2021, Hamilton Beach began notifying customers and state Attorneys General about a data breach that occurred from December 18, 2020 to February 4, 2021 (the "Data Breach"). Hackers not only "scraped" many of Hamilton Beach's customers' names from Defendant's website by infecting the ecommerce platform with malware, hackers also stole customers' payment card numbers, CVV security codes, credit card expiration dates, addresses, telephone numbers and email addresses ("PII"). The criminals obtained everything they needed to illegally use Hamilton Beach customers' payment cards to make fraudulent purchases, and to steal the customers' identities.

3. Not only did hackers skim Hamilton Beach's customers' PII, on information and belief, the stolen names and payment card information are now for sale on the dark web. That means the Data Breach worked. Hackers accessed and then offered for sale the unencrypted, unredacted, stolen PII to criminals. Because of Defendant's Data Breach, customers' PII is still available on the dark web for criminals to access and abuse. Hamilton Beach's customers face a lifetime risk of identity theft.

4. All of this personally identifiable information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect customers' data.

5. The stolen PII has great value to hackers: More than 6000 customers were affected by the Data Breach. For example, Hamilton Beach has filed data breach notices in California, Maine, and Montana, among others.[1]

6. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect its users' PII, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor Defendant's websites and ecommerce platforms for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

7. Plaintiff and similarly situated Hamilton Beach customers ("Class Members") have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under New York's General Business Law; and (v) the continued and certainly an increased risk to their PII, which: (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendant's possession

[1] *See, e.g.,* Hamiton Beach's *Notice of Data Breach,* archived by the Maine Attorney General on April 9, 2021, *available at*: https://apps.web.maine.gov/online/aeviewer/ME/40/6f16923d-a302-4580-b0ba-2e1037da54e4/001dbb92-e231-4306-ad14-4b1b9206f750/document.html, last accessed April 22, 2021.

and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

PARTIES

8. Plaintiff Carrie Koval-Burt is a citizen of New York residing in Westchester County, New York. Ms. Koval-Burt purchased Hamilton Beach products from Defendant's website on January 10, 2021, using her family's Citibank credit card. She received Hamilton Beach's' *Notice of Data Breach* or about April 9, 2021.

9. Defendant Hamilton Beach Brands, Inc. is a Delaware corporation with its principal place of business at 4421 Waterfront Drive, Glen Allen, VA. Hamilton Beach advertises and sells goods to residents nationwide through its website and various retailers.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Moreover, this Court has jurisdiction over this action under 28 U.S.C. § 1332(a)(1) because Plaintiff is a New York citizen and therefore diverse from Defendant, which is not a New York citizen.

11. This Court has personal jurisdiction over Defendant because Defendant is a Delaware corporation with its principal place of business within this District.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

13. Hamilton Beach has existed in various forms since 1910 as a manufacturer of

kitchen appliances.[2] Today it markets its appliances both on its own website as well as through major retailers, including Macy's and Amazon.com.

14. Customers purchasing online demand security to safeguard their PII. Hamilton Beach touts the secure nature of its website in its Privacy Policy:

> Hamilton Beach Brands, Inc., its subsidiaries and divisions (collectively, the "Company," "we," or "us") believe that privacy is important and we are committed to maintaining the trust of our customers and our online guests.
>
> …
>
> **How We Protect Your Information**
>
> We will not use your personal information for any purpose other than the purposes described in this Privacy Policy.
>
> We use reasonable security measures, including physical, administrative, and technical safeguards to help us protect your information from unauthorized access, use and disclosure. These measures may include encryption, security certificates, access controls, information security technologies, policies, procedures and other information security measures to help protect your information. We also require our suppliers to protect such information from unauthorized access use and disclosure. [3]

15. The PCI DSS (Payment Card Industry Data Security Standard) compliance is a requirement for businesses that store, process, or transmit payment card data. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions.

16. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: Developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks using anti-virus software and updating it regularly.[4]

17. To purchase products on Hamilton Beach's website, customers can create an account or check out as a guest. To complete a purchase, at a minimum, the customer must enter

---

[2] *See* https://www.hamiltonbeachbrands.com/about-our-company/our-history/default.aspx, last accessed April 22, 2021.
[3] https://hamiltonbeach.com/privacy-policy, last accessed April 22, 2021.
[4] PCI Security Standards Council, *available at*: https://www.pcisecuritystandards.org/, last accessed April 22, 2021.

the following PII:

- Name;
- billing address;
- delivery address;
- email address;
- telephone number;
- name on the payment card;
- type of payment card;
- full payment card number;
- payment card expiration date; and
- security code, or CVV code (card verification number).

18. At no time during the final checkout process does Hamilton Beach require customers to expressly agree to "Terms of Use," "Terms of Service" or "Terms & Conditions."

The Data Breach

19. Beginning on or about April 9, 2021, Hamilton Beach sent customers a *Notice of Data Breach* signed by Senior Manager of Digital Marketing Chuck Vion.[5] Vion informed the recipients of the notice that:

> **What Happened?**
> On February 4, 2021, Hamilton Beach discovered unauthorized computer code on its ecommerce website (www.hamiltonbeach.com). We immediately removed the unauthorized code, began an investigation, and a cybersecurity firm was engaged to assist with our investigation. The code was capable of obtaining information entered by customers during the checkout process and sending that information out of our system. On March 12, 2021, the investigation determined that an unauthorized person could have accessed information entered by some customers during the checkout process for orders attempted or placed between December 18, 2020 and February 4, 2021.
>
> **What Information Was Involved?**
> The information that could have been copied was: Contact Information – first and last name, shipping and billing address, email address, and phone number; Payment card information – payment card number, expiration date, and card verification code for the payment card. . .

20. Hamilton Beach's customers' information is likely for sale on the dark web and, on information and belief, is still for sale to criminals. This means that the Data Breach was successful; unauthorized individuals accessed Hamilton Beach's customers' unencrypted,

[5] Available at https://apps.web.maine.gov/online/aeviewer/ME/40/6f16923d-a302-4580-b0ba-2e1037da54e4.shtml, last accessed April 22, 2021

unredacted information, including "Name; Street Address; City; State; Zip/Postal Code; Country; Phone Number; Email Address; Payment Card Number; Payment Card Security Code; and Payment Card Month/Year of Expiration," and possibly more, without alerting Defendant, then offered the "scraped" information for sale online. There is no indication that Defendant's customers' PII was removed from the dark web where it likely remains.

21. Not long before Hamilton Beach admitted hackers were scraping its customers' PII, the FBI issued yet another warning to companies about this exact type of fraud. In the FBI's *Oregon FBI Tech Tuesday: Building a Digital Defense Against E-Skimming*, dated October 22, 2019, the agency stated:

> This warning is specifically targeted to . . . businesses . . . that take credit card payments online. E-skimming occurs when cyber criminals inject malicious code onto a website. The bad actor may have gained access via a phishing attack targeting your employees—or through a vulnerable third-party vendor attached to your company's server.

22. The FBI gave some stern advice to companies like Hamilton Beach:

> Here's what businesses and agencies can do to protect themselves:
>
> - Update and patch all systems with the latest security software.
> - Anti-virus and anti-malware need to be up-to-date and firewalls strong.
> - Change default login credentials on all systems.
> - Educate employees about safe cyber practices. Most importantly, do not click on links or unexpected attachments in messages.
> - Segregate and segment network systems to limit how easily cyber criminals can move from one to another.

23. But Defendant apparently did not take this advice: hackers scraped customers' PII off its website—and continued to do so until at least February 4, 2021.

24. Web scraping or skimming data breaches are commonly made possible through a vulnerability in a website or its backend content management system. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were collecting, causing customers' PII to be exposed and sold on the dark web.

Scraping and E-Skimming Breaches

25. *Magecart* is a loose affiliation of hacker groups responsible for skimming payment card attacks on various companies, including British Airways and Ticketmaster.[6] Typically, these hackers insert virtual credit card skimmers or scrapers (also known as *formjacking*) into a web application (usually the shopping cart), and proceed to scrape credit card information to sell on the dark web.[7]

26. The hackers target what they refer to as the *fullz*–a term used by criminals to refer to stealing the full primary account number, card holder contact information, credit card number, CVC code, and expiration date. The *fullz* is exactly what Hamilton Beach admits the malware infecting its ecommerce platform scraped.

27. These cyber-attacks exploit weaknesses in the code of the ecommerce platform, without necessarily compromising the victim website's network or server. These attacks often target third-party payment processors like Shopify and Salesforce.

28. Unfortunately, despite all of the publicly available knowledge of the continued compromises of PII in this manner, Defendant's approach to maintaining the privacy and security of Plaintiff's and Class members' PII was negligent, or, at the very least, Defendant did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect its customers' valuable PII.

29. The Data Breach is compounded by the fact that this is not Defendant's first data beach of customer PII. On or about January 28, 2011, Defendant disclosed that its e-commerce site had been infiltrated by hackers and compromised.[8]

---

[6] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost, Aug. 28, 2019, *available at*: https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/, last accessed April 22, 2021.

[7] *Id*.

[8] *Hamilton Beach Reports Hack; Credit Card Data at Risk*, DarkReading, January 28, 2011, available at https://www.darkreading.com/attacks-breaches/hamilton-beach-reports-hack-credit-card-data-at-risk/d/d-id/1135122, last accessed April 22, 2021.

Value of Personally Identifiable Information

30. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Experian reports that a stolen credit or debit card number can sell for $5-110 on the dark web; the *fullz* sold for $30 in 2017.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

31. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

32. Defendant was, or should have been, fully aware of the significant volume of daily credit and debit card transactions on its website, amounting to thousands of payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

Plaintiff Koval-Burt's Experience

33. Plaintiff Carrie Koval-Burt purchased a product from Hamilton Beach's website on January 10, 2021. She checked out as a guest and used her family's Citibank credit card.

34. On the payment platform, Ms. Koval-Burt entered her PII: name, billing address, delivery address, payment card type and full number, CVV security code, payment card expiration date, and email address. During this transaction, Ms. Koval-Burt was not asked to "agree" to any "Terms of Service" or to review the "Privacy Policy."

---

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/, last accessed April 22, 2021.

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/, last accessed April 22, 2021.

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/, last accessed April 22, 2021.

35. From February 23 to March 1, 2021, a series of five unauthorized purchases totaling $233.43 were made on the card. Citibank confirmed on March 1 and March 2, 2021, that her card had been used by unauthorized third-parties multiple times.

36. Citibank changed the account number in response to the illegal charges and mailed her a new card. Ms. Koval-Burt and her spouse had to take time out of her day to deal with the fraudulent charges and the account number change, as well as to change recurring charges that would otherwise be made on the card. This was time they otherwise would have spent performing other activities, such as their jobs and/or leisurely activities for the enjoyment of life. They also had to use alternative methods of payment until they received their new credit card.

37. On or about April 9, 2021, Hamilton Beach notified Ms. Koval-Burt by U.S. mail of the Data Breach in the *Notice of Data Breach*. She did not receive notice by email.

38. In response to the *Notice of Data Breach*, Ms. Koval-Burt and her spouse again had to spend time dealing with the consequences of the Data Breach, which includes time reviewing the account compromised by the Data Breach (which was her Citibank credit card), contacting their bank, exploring credit monitoring options, and self-monitoring her accounts. This is time Ms. Koval-Burt otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

39. Knowing that the hacker stole her PII, and that her PII may be available for sale on the dark web, has caused Ms. Koval-Burt great concern. She is now very concerned about credit card theft and identity theft in general. This breach has given Ms. Koval-Burt hesitation about using Hamilton Beach's services, and reservations about shopping on other online websites.

40. Now, due to Defendant's misconduct and the resulting Data Breach, hackers obtained her PII at no compensation to Ms. Koval-Burt whatsoever. That is money lost for her, and money gained for the hackers – who could sell her PII on the dark web.

41. Ms. Koval-Burt also suffered actual injury and damages in paying money to, and purchasing products from, Defendant's website during the Data Breach, expenditures which she would not have made had Defendant disclosed that it lacked computer systems and data security

practices adequate to safeguard customers' PII from theft.

42. Moreover, Ms. Koval-Burt suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

43. Plaintiff Koval-Burt has a continuing interest in ensuring her PII, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Koval-Burt's Efforts to Secure PII

44. Defendant's Data Breach caused Ms. Koval-Burt harm.

45. Prior to the activity described above during the period in which the Data Breach occurred, the Citibank credit card that Ms. Koval-Burt used to purchase products on Defendant's website had never been stolen or compromised. Ms. Koval-Burt and her spouse reviewed their credit reports and other financial statements routinely and to her knowledge this card had not been compromised in any manner.

46. Additionally, Ms. Koval-Burt never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

47. Ms. Koval-Burt stores any and all electronic documents containing her PII in a safe and secure location, and destroys any documents she receives in the mail that contain any of her PII, or that may contain any information that could otherwise be used to compromise her credit card.

CLASS ALLEGATIONS

48. Plaintiff brings this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All individuals whose PII was compromised in the data breach announced by Hamilton Beach on April 9, 2021 (the "Nationwide Class").

49. The New York Subclass is defined as follows:

> All persons residing in New York whose PII was compromised in the data breach

announced by Hamilton Beach on April 9, 2021 (the "New York Subclass").

50. Excluded from the Class are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to Defendant's departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as Defendant's immediate family members.

51. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

52. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has identified thousands of customers whose PII may have been improperly accessed in the data breach, and the Classes are apparently identifiable within Defendant's records.

53. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class members. These include:

a. When Defendant actually learned of the data breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class members' PII;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class members' PII;

f. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent loss or

misuse of that PII;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

h. Whether Defendant caused Plaintiff and Class members damages;

i. Whether Defendant violated the law by failing to promptly notify Class members that their PII had been compromised;

j. Whether Plaintiff and the other Class members are entitled to credit monitoring and other monetary relief;

k. Whether Defendant violated New York's General Business Law (N.Y.G.B.L. § 349, et seq.).

54. **Typicality**: Plaintiff's claims are typical of those of other Class members because all had their PII compromised as a result of the data breach, due to Defendant's misfeasance.

55. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class members. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

56. **Superiority and Manageability**: Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

57. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

58. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification

because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach; and

e. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

59. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 58.

60. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

61. The legal duties owed by Defendant to Plaintiff and Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class members in its possession;

b. To protect PII of Plaintiff and Class members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the data breach.

62. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendant.

63. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Class members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

64. Defendant breached its duties to Plaintiff and Class members. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the facts that "scraping" hacks have been surging since 2016.

65. Defendant knew or should have known that its security practices did not adequately safeguard Plaintiff's and the other Class members' PII, including, but not limited to, the failure to detect the malware infecting Defendant's ecommerce platform for months.

66. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII during the period it was within Defendant's possession and control.

67. Defendant breached the duties it owes to Plaintiff and Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the data breach (*e.g.,* there is no indication that Defendant's ecommerce platform is PCI DSS compliant and encrypts customers' order information, such as name, address, and credit card number, during data transmission, which did not occur here);

c. Failing to act despite knowing or having reason to know that Defendant's systems were vulnerable to E-skimming or similar attacks (*e.g.*, Defendant did not detect the malicious code on the ecommerce platform, nor did it implement safeguards in light of the surge of E-skimming attacks on retailers); and

d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

68. Due to Defendant's conduct, Plaintiff and Class members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used in identity theft and other types of financial fraud against the Class members. Hackers not only "scraped" many of Hamilton Beach's customers' names from the website, they also stole customers' billing and shipping addresses, payment card numbers, CVV codes, and payment card expiration dates. They got the *fullz* – everything they need to illegally use Hamilton Beach's customers' credit cards to make illegal purchases. There is no question that this PII was taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

69. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach.[12] Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

70. As a result of Defendant's negligence, Plaintiff and Class members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession, subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiff and Class members, including ongoing credit monitoring.

71. These injuries were reasonably foreseeable given the history of security breaches of this nature since 2011. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's negligent conduct.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

72. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 58.

[12] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring, but it only monitors victims' credit reports at one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

73. When Plaintiff and Class members provided their PII to Defendant in exchange for Defendant's products, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their PII.

74. Defendant solicited and invited Plaintiff and Class members to provide their PII as part of Defendant's regular business practices and as essential to the sales transaction process for card payment transactions. This conduct thus created implied contracts between Plaintiff and Class members on one hand, and Defendant on the other hand. Plaintiff and Class members accepted Defendant's offer by providing their PII to Defendant in connection with their purchases from Defendant.

75. When entering into these implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

76. Defendant's implied promise to safeguard Plaintiff's and Class members' PII is evidenced by a duty to protect and safeguard PII that Defendant required Plaintiff and Class members to provide as a condition of entering into consumer transactions with Defendant.

77. Plaintiff and Class members paid money to Defendant to purchase products or services from Defendant. Plaintiff and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

78. Plaintiff and Class members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from customers' continued use of Defendant's website—that Defendant would adequately safeguard PII. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Class members.

79. Plaintiff and Class members value data security and would not have provided their PII to Defendant in the absence of Defendant's implied promise to keep the PII reasonably secure.

80. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendant.

81. Defendant breached their implied contracts with Plaintiff and Class members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

82. As a direct and proximate result of Defendant's breach of the implied contract, Plaintiff and Class members sustained damages as alleged herein.

83. Plaintiff and Nationwide Class members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

84. Plaintiff and Class members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

THIRD CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class)

85. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 58.

86. Defendant owes duties of care to Plaintiff and Class members which would require it to adequately secure PII.

87. Defendant still possesses PII regarding Plaintiff and Class members.

88. Although Hamilton Beach claims in its *Notice of Data Breach* that it had "ensure[d] the unauthorized person was no longer able to collect customer information and are taking measures to enhance the security of our site," there is no detail on what, if any, fixes have occurred.

89. Plaintiff and Class members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

90. There is no reason to believe that Defendant's security measures are any more adequate than they were before the breach to meet Defendant's contractual obligations and legal duties, and there is no reason to think Defendant has no other security vulnerabilities that have not yet been knowingly exploited.

91. Plaintiff, therefore, seeks a declaration that (1) each of Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and securing checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and Class members for a period of ten years; and

h. Meaningfully educating its users about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendant's customers must take to protect themselves.

FOURTH CLAIM FOR RELIEF
Violation of New York General Business Law § 349, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class, or, in the alternative, On Behalf of Plaintiff and the New York Subclass)

92. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 58.

93. New York's General Business Law § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce.

94. In its provision of services throughout the State of New York, Defendant conducts business and trade within the meaning and intendment of New York's General Business Law § 349.

95. Plaintiff and members of the Class are consumers who conducted transactions with Defendant for their personal use.

96. By the acts and conduct alleged herein, Defendant has engaged in deceptive, unfair, and misleading acts and practices, which include, without limitation, misrepresenting that Defendant used "reasonable physical, technical and administrative measures to protect Personal Information under our control" when in fact Defendant did not.

97. The foregoing deceptive acts and practices were directed at consumers.

98. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the ability and measures taken by Defendant to safeguard consumer PII, and to induce consumers to enter transactions with Defendant.

99. By reason of this conduct, Defendant engaged in deceptive conduct in violation of GBL § 349.

100. Defendant's actions are the direct, foreseeable, and proximate cause of the damages that Plaintiffs and members of the Classes have sustained from having provided their PII to Defendant, which was exposed in the data breach.

101. As a result of Defendant's violations, Plaintiff and members of the Classes have suffered damages because: (a) they would not have provided their PII to Defendant had they known Defendant did not use "reasonable security measures, including physical, administrative, and technical safeguards to help us protect your information from unauthorized access, use and disclosure"; (b) they have suffered identity theft and/or fraudulent charges and their PII has been devalued as a result of being exposed in the data breach; and (c) Plaintiff and members of the Classes must spend considerable time and expenses dealing with the effects of the data breach, and are now at greater risk for future harm stemming from the data breach.

102. On behalf of themselves and other members of the Classes, Plaintiff seek to recover their actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

103. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 58.

104. Plaintiff and class members conferred a monetary benefit upon Defendant in the form of monies paid for goods available on Defendant's websites.

105. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendant also benefited from the receipt of Plaintiff's and Class members' PII, as this was used by Defendant to facilitate payment to them.

106. The monies for goods that Plaintiff and Class members paid to Defendant were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

107. As a result of Defendant's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class members

paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

108. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

109. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received by it as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all Class members, requests judgment against the Defendant and that the Court grant the following:

A. An order certifying the Nationwide Class and New York Subclass as defined herein, and appointing Plaintiff and their counsel to represent the classes;

B. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class members' PII;

C. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiff and all Class members;

D. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 26, 2021

Respectfully Submitted,

/s/ Steven T. Webster

Steven T. Webster (VSB No. 31975)
Webster Book LLP
300 N. Washington St., Suite 404
Alexandria, VA 22314
Telephone and Fax: (888) 987-9991
swebster@websterbook.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Carl Malmstrom
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 545-4653
malmstrom@whafh.com